

WHAT IS CLAIMED IS:

- 1                    1. A method of signing digital data, comprising the steps of:
- 2                        subjecting the data to be signed to a message digest function to produce a
- 3     digest of the data to be signed;
- 4                        transmitting the message digest to a small, mobile transaction device which
- 5     contains a secret key and a user's PIN code;
- 6                        determining whether a user's PIN code is correct and, if it is, hashing the digest
- 7     as a function of said secret key;
- 8                        returning the transformed message digest to a service provider;
- 9                        digesting and hashing the original data at the service provider using the same
- 10     message digest function and secret key; and
- 11                        determining whether the hashed message digest at the service provider matches
- 12     the hashed message digest received from the transaction device.